

Scopus

Document details

[Export](#) [Download](#) [Print](#) [E-mail](#) [Save to PDF](#) [Add to List](#) [More... >](#)
[Full Text](#)[View at Publisher](#)

Proceedings - 5th International Conference on Computer and Communication Engineering: Emerging Technologies via Comp-Unication Convergence, ICCCE 2014

4 February 2015, Article number 7031600, Pages 60-63

5th International Conference on Computer and Communication Engineering, ICCCE 2014; Sunway Putra HotelKuala Lumpur; Malaysia; 23 September 2014 through 24 September 2014; Category numberE5413; Code 110844

A secure authentication scheme for Bluetooth connection (Conference Paper)

Diallo, A.S. [✉](#), Wajdi, A. [✉](#), Olanrewaju, R.F. [✉](#), Sado, F. [✉](#)

[View additional authors](#) [v](#)

Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, P.O. Box 10, Kuala Lumpur, Malaysia

[View additional affiliations](#) [v](#)

Abstract

Recently, Bluetooth technology is widely used by organizations and individuals to provide wireless personal area network (WPAN) because the radio frequency (RF) waves can easily penetrate obstacles and can propagate without direct line-of-sight (LoS). However, there are serious security challenges associated with wireless communication systems since they are easier to eavesdrop, disrupt and jam than the wired systems. Bluetooth technology uses either legacy pairing or secure and simple pairing (SSP), however both are vulnerable to attacks such as eavesdropping and man-in-the-middle (MITM) attacks. Therefore, this paper has proposed a secure protocol that uses a double encryption to identify the slave. The implementation of this proposal is based on the Arduino Integrated Development Environment (IDE) as software and a Bluetooth (BT) Shield connected to an Arduino Uno R3 boards as hardware. The result was verified on a Graphical User Interface (GUI) built in Microsoft Visual Studio 2010. It has shown that the proposed scheme works perfectly and the protocol thwarts the passive and active eavesdropping which exist during SSP. These attacks are defeated by avoiding the exchange of passwords and public keys in plain text. Therefore, this protocol is expected to be implemented by the Bluetooth Specification Interest Group (SIG) to enhance the security in Bluetooth connection. © 2014 IEEE.

Author keywords

authentication Bluetooth security legacy pairing secure and simple pairing

Indexed keywords

Engineering
controlled terms:

Authentication Cryptography Graphical user interfaces Mobile security Network security
Personal communication systems Security systems User interfaces Web services
Wireless telecommunication systems

Metrics [①](#)

5 Citations in Scopus

Field-Weighted

Citation Impact

Cited by 5 documents

Wearable devices

Wanjari, N.D. , Patil, S.C.
(2017) *2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology, ICAECCT 2016*

Security enhancement of wireless sensor networks using signal intervals

Moon, J. , Jung, I.Y. , Korea, J.Y.
(2017) *Sensors (Switzerland)*

Design of BLE key agreement scheme based on hash chain

Huang, Y. , Huang, Y. , Yu, B.
(2016) *Xitong Fangzhen Xuebao / Journal of System Simulation*

[View all 5 citing documents](#)

Inform me when this document is cited in Scopus:

[Set citation alert >](#)

[Set citation feed >](#)

Related documents

Find more related documents in Scopus based on:

[Authors >](#) [Keywords >](#)

Bluetooth
specification

Graphical user
interfaces (GUI)

Integrated
development
environment

legacy pairing

Man in the middles
(MITM)

secure and simple
pairing

Wireless
communication
system

Wireless personal
area networks

Engineering main heading: Bluetooth

ISBN: 978-147997635-5	DOI: 10.1109/ICCCE.2014.29
Source Type: Conference Proceeding	Document Type: Conference Paper
Original language: English	Volume Editors: Gunawan T.S.
	Sponsors: Felda Wellness Corporation,Malaysia Convention and Exhibition Bureau (MyCEB),Malaysian Industry-Government Group for High Technology,University Putra Malaysia,Yayasan Kesejahteran Bandar
	Publisher: Institute of Electrical and Electronics Engineers Inc.

© Copyright 2015 Elsevier B.V., All rights reserved.

^ Top of page